A Comprehensive Framework to Simulate Network Attacks and Challenges

Egemen K. Çetinkaya, Dan Broyles, Amit Dandekar, Sripriya Srinivasan, James P. G. Sterbenz
Information and Telecommunication Technology Center, The University of Kansas
Lawrence, Kansas, USA
{ekc, dbroyl01, dandekar, sripriya, jpgs}@ittc.ku.edu

***Abstract*—Communication networks have evolved tremendously over the past several decades, offering a multitude of services while becoming an essential critical infrastructure in our daily lives. Networks in general, and the Internet in particular face a number of challenges to normal operation, including attacks and large-scale disasters, as well as due to the characteristics of the mobile wireless communication environment. It is therefore vital to have a framework and methodology for understanding the impact of challenges to harden current networks and improve the design of future networks. In this paper, we present a framework to evaluate network dependability and performability in the face of challenges. This framework uses ns-3 simulation as the methodology for analysis of the effects of perturbations to normal operation of the networks, with a challenge specification applied to the network topology. This framework can simulate both static and dynamic challenges based on the failure or wireless-impairment of individual components, as well as modelling geographically-correlated failures. We demonstrate this framework with the Sprint Rocketfuel and synthetically generated topologies as well as a wireless example, to show that this framework can provide valuable insight for the analysis and design of resilient networks.**

***Keywords*-Internet resilience, survivability, dependability, performability; challenge, attack, disaster, correlated failure; network topology, critical infrastructure; ns-3 simulation, modelling**

I. Introduction and Motivation

Communication networks have evolved tremendously over the past several decades, offering a multitude of services while becoming an essential critical infrastructure in our daily lives. While this evolution is still progressing, user expectations from these networks increases in terms of performance and dependability. On the other hand, achieving fully resilient networks is practically impossible, in part due to cost constraints, and therefore networks experience disruptions. We define *resilience* as the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operations [1]; resilience is a discipline that subsumes survivability, fault tolerance, disruption tolerance, dependability, and performability.

Understanding network behaviour under perturbations can improve today's networks performance, as well as lead to more resilient and survivable future networks. Therefore, it is essential to have a through understanding of the network behaviour when exposed to challenges, such as component failures, attacks, large-scale disasters, and effects of the mobile wireless communication environment.

Understanding network disruptions and their cause is crucial for planning and designing the networks. Some challenges to the network are inherent in the communication environment, in particular the weak connectivity of wireless channels and the dynamic behaviour due to mobility. Attacks against the network are frequent, and there are also challenges caused by acts of nature such as hurricanes and solar storms. Additionally, networks are built by humans and are not completely resilient due to design flaws and cost constraints. The redundancy and diversity that increase resilience add to the cost of the network. Therefore, we need to understand the challenges that are inherent in the communication environment, and their impact on network operation and the service delivered to users.

We cannot thoroughly study the effects of challenges in live networks without impacting users. Testbeds are useful, but do not provide the scope and scale necessary to understand the resilience of large, complex networks, although progress is being made in this direction [2]. Simulations arguably provide the best compromise between tractability and realism to study challenges that are inherent in the communication environment, however this is nontrivial [3].

In this paper, we present a framework to understand the network behaviour when faced by challenges to communication networks. Different forms of challenges impose varying impacts, therefore they need to be modelled accordingly. As a result, we present models to represent the various forms of challenges and present example simulation results of network performance when exposed to examples of such challenges.

The rest of the paper is organised as follows: We present challenges in communication networks and categorise them in Section II. The evaluation methodology and implementation of challenge models are presented in Section III, followed by the demonstrative results in Section IV. Lastly, we summarise our findings as well as propose future work in Section V.

II. Network Challenge Models

A *challenge* is an event that impacts normal operation [1]. A challenge triggers *faults*, which are the hypothesised cause of errors. Eventually, a fault may manifest itself as an error. If the error propagates it may cause the delivered services to fail [4]. Challenges to the normal operation of networks include unintentional misconfiguration or operational mistakes, malicious attacks, large-scale natural disasters, and environmental

978-1-4244-7286-4/10/$26.00

challenges [1], [5]. Network challenges can be categorised based on intent, scope, and domain they impact. The network challenge taxonomy used for the simulation framework is shown in Figure 1.

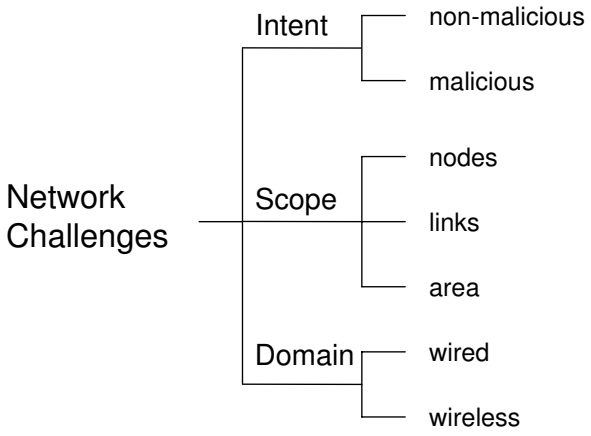


Fig. 1. Taxonomy of network challenges

It is essential to differentiate the challenges exposed and understand their impact. Next, we present the modelling of various challenges, for this paper grouped into three coarse categories: intent, scope, and domain.

A. Challenge Models Based on Intent

We model the challenges based on the intent as non-malicious or malicious. Non-malicious challenges can be due to incompetence of an operator (e.g. accidental fiber cut, misconfiguration of network resources) or designer (e.g. hardware or software faults eventually causing a node or a link to fail). These random events affect node and link availability, and result in the majority of the failures observed [6]–[8]. On the other hand, malicious attacks, orchestrated by an intelligent adversary, target *specific* parts of a network and can have significant impact if critical elements of the network fail.

B. Challenge Models Based on Scope

Scope of a challenge can be further categorised based on nodes, links, or network elements affected within a geographic area. While node and link failures can impact a single or multiple network elements, area-based challenges usually affect multiple network elements. Natural phenomenon that are geographically correlated can impact quite large areas. Hurricanes, earthquakes, and solar storms are examples of natural disasters that can impact the network at a large scale [9]–[11]. Furthermore, geographically correlated failures can be due to dependency among the critical infrastructures, as recently experienced in the 2003 Northeast blackout in the US [12], [13].

C. Challenge Models Based on Domain

Networks have quite different characteristics based on the wired and wireless domain in which they operate. Communication network performance in the wireless domain is primarily affected by the mobility of the nodes and the impairments caused by the wireless medium. The challenges that are inherent in the wireless domain include weakly connected channels, mobility of nodes in an ad-hoc network, and unpredictably long delays [5]. These are the natural result of noise, interference, and other effects of RF propagation such as scattering and multipath, as well as the mobility of wireless nodes. Furthermore, weather events such as rain and snow can cause the signals to attenuate and impairs the wireless communication network [14]. Malicious nodes may jam the signal of legitimate users to impair communication in the open wireless medium.

While the above-mentioned challenge models are orthogonal to each other, challenge scenarios are a combination of challenge sub-categories. For example, a failure due to natural aging of a component can be categorised as a non-malicious, wired (or wireless), node failure.

III. Simulation Framework

In this section, we present our simulation framework to evaluate the resilience of network topologies when subject to a variety of challenges.

A. Methodology Overview

Simulation via abstraction is one of the techniques to analyse networks in a cost-effective manner. We have chosen the ns-3 [15] network simulator since it is open source, flexible, provides mixed wired and wireless capability (unlike ns-2), and the models can be extended. Unfortunately, the simulation model space increases multiplicatively with the different number of challenges and network topologies being simulated. Hence, for n different topologies subjected to c different challenges, $n \times c$ models have to be generated and simulated. The proposed framework decouples the challenge generation from topologies by providing a comprehensive challenge specification framework, thereby reducing the simulation model space to $n + c$. We have created an automated simulation model generator that arbitrarily combines network topologies and challenge specifications, thus increasing the efficiency of simulation generation. Our simulation framework consists of four distinct steps as shown in Figure 2.

The first step is to provide a challenge specification that includes the type of the challenge and specifics of the challenge type. The second step is to provide a description of the network topology, consisting of node geographical or logical coordinates and an adjacency matrix. The third step is the automated generation of ns-3 simulation code based on the topology and challenge descriptor. Finally, we run the simulations and analyse the network performance under challenge scenarios. Additionally, the simulation framework can also be enabled to generate ns-3 network animator (NetAnim) traces for visualisation purposes. A NetAnim screenshot of Rocketfuel [16] inferred Sprint backbone network topology of 27 nodes and 68 links is shown in Figure 3.

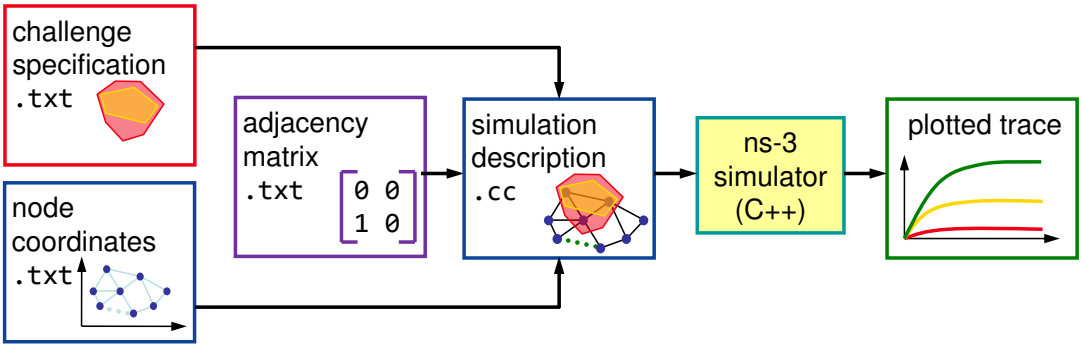


Fig. 2. Framework flow diagram

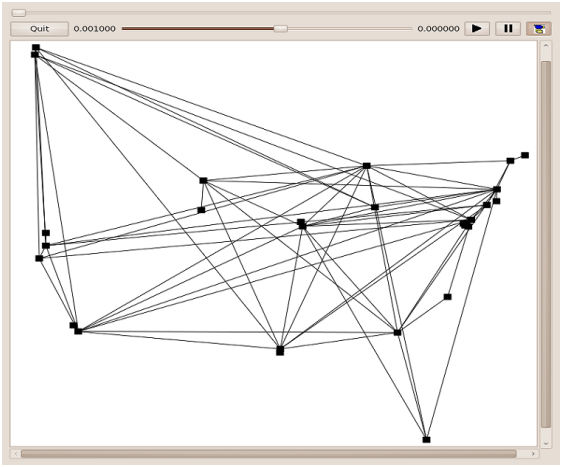


Fig. 3. NetAnim screenshot of inferred Sprint topology

B. Implementation of Challenge Models

Modelling and simulating network performance under challenge conditions is non-trivial [3]. There have been several studies that analyse different aspects of networks under challenges, however to the best of our knowledge, this is the first unified framework that models a wide range of challenges.

1) Non-malicious challenges: In the case of wired domain challenges in this category, the number of nodes or links k and challenge period is specified in the challenge specification file. This type of challenge models failures that are uncorrelated with respect to topology and geography, e.g. random node and link failures. Network topologies faced by random node or link failures have been studied [17], [18].

2) Malicious attacks: We use topological properties of the graph in order to determine the *critical* elements in the network such as the degree of connectivity of nodes and betweenness of nodes and links (betweenness is the number of shortest paths through a particular element [19]). The critical nodes or links are shut down for the duration of the challenge period. Topological characteristics of the networks have been studied under attacks based on degree of connectivity and betweenness centrality of the nodes and links [20]–[23].

3) Large-scale disasters: The challenge specification for area-based challenges is an n-sided polygon with vertices located at a particular set of geographic coordinates or a circle centered at a user specified coordinates with radius r. The simulation framework then determines the nodes and links that are encompassed by the polygon or circle, and disables them during the challenge interval. We use the Computational Geometry Algorithms Library (CGAL) [24], which is an open source library with efficient geometric algorithms implemented in C++. We also implement dynamic area-based challenges, in which challenge area can evolve in shape over time: scale (expand or contract), rotate, and move on a trajectory during the simulation. Large-scale regional failure scenarios previously only have been modelled as a static circle [25] for evaluating the performance of path restoration after a failure. Examples of the need to simulate arbitrary polygons are to model large-scale power blackouts and large-scale natural disasters such as hurricanes.

4) Wireless challenges: To simulate challenges in wireless domain, we create a new propagation loss model that includes a mobility model parameter and range of influence. Using these parameters, the user can specify where the loss takes place and how it moves over time. In this way, we model a realistic challenge instead of relying solely upon statistical methods. Unlike signal loss due to scattering and line-of-sight obstacles, jammers can cause radio channel interference that increase channel noise and reduce the signal to noise ratio that is critical to a receiver's ability to discern the data bits correctly. We implement a jammer module that sends high power signals with high data rate packets continuously on the same channel. A toolkit was previously implemented in ns-2 for simulating obstacles, however it lacks jammers and impairments [26].

IV. Example Simulations

In this section, we apply our challenge framework and evaluation methodology to sample topologies to demonstrate the utility of this approach. The ns-3 simulation parameters are as follows: The network is composed of bidirectional wired links with 10 Mb/s bandwidth and 2 ms transmission delay. Routing is accomplished using the Dijkstra shortest path first

algorithm, recalculated at each time step, with reconvergence delay as a simulation parameter. The traffic is constant bit rate (CBR) at 40 kb/s between every node pair, with 1000 Byte packets. These parameters are chosen such that there is no congestion under normal operation, but the network is not significantly over-provisioned so that we will see the effect of node and link failures. We measure the network's performance under challenges in terms of packet delivery ratio (PDR).

A. Non-malicious and Malicious Challenges

First, we evaluate the performance of three separate topologies shown in Figure 4 under the presence of malicious and non-malicious challenges. The topologies we choose are the Sprint inferred topology (Figure 4a) and two synthetic topologies (Figure 4b and 4c). The synthetic topologies are generated using the KU-LoCGen topology generation tool [27], [28]. KU-LoCGen generates topologies with geographic constraints and places links between nodes using the modified Waxman [29] model. The resulting synthetic topologies have the same number of nodes at the same geographic locations as the inferred Sprint topology, however the number of links and connectivity of the nodes differ. The two synthetic graphs chosen for this paper consist of a richly connected and poorly connected topology to demonstrate the range of robustness results from this simulation framework. The graph characteristics of three topologies are presented in Table I.

TABLE I
TOPOLOGICAL CHARACTERISTICS OF SAMPLE NETWORKS

Network Topology	Sprint	Synthetic 1	Synthetic 2
Number of nodes	27	27	27
Number of edges	68	74	68
Maximum degree	12	9	10
Average degree	5.04	5.5	5.04
Clustering coeff.	0.43	0.29	0.38
Network diameter	6	4	6
Average hopcount	2.44	2.2	2.9
Node betweenness (max/min/avg)	144/28/72	76/2/36.8	302/2/269.9
Link betweenness (max/min/avg)	72/2/12.6	31/1/10.5	140/1/14.9

We evaluate the performance of the sample topologies under the presence of malicious and non-malicious challenges with the PDR of the network shown in Figure 5 for link failures and in Figure 6 for node failures with up to 10 links or nodes down. We measure the instantaneous PDR at the steady-state condition during the challenges for each point. We also note that for random failures, we averaged the results over 100 runs. For malicious challenges (betweenness or degree of connectivity), first we calculate the betweenness (or degree of connectivity) for each network element in the topology, and provide the challenge file as the list of the elements to be brought down.

Figure 5 shows the PDR during the link perturbations to Sprint inferred (Figure 5a), synthetic 1 (Figure 5b), and synthetic 2 (Figure 5c) topologies respectively. We evaluate the PDR during link failures for two cases: 10 random link failures and an attack using the 10 highest ranked links based on link betweenness values. Except for the synthetic topology 1, link attacks have more degrading impact than the random failures. The PDR of 100% for both random and attack cases for the synthetic 1 topology (Figure 5b) can be attributed to this topology's lower average hop count, network diameter, clustering coefficient, and higher average degree. The synthetic topology 1 also has six more links compared to the other two topologies: 74 vs. 68. On the other hand, the link attack on highest betweenness link for synthetic topology 2 results in a PDR drop to 60%. Visual inspection of synthetic topology 2 (Figure 4c) clearly identifies the link cut between the central and west US is the cause of such high drop since the network partitions after the link failure. We can also infer the same conclusion by examining the link betweenness of synthetic topology 2 in Table I, in which this link has 140 shortest paths.

The performance of sample topologies against non-malicious and malicious node perturbations is shown in Figure 6. We evaluate the PDR during node failures for three cases: 10 random node failures, attack of 10 highest ranked nodes based on betweenness, and attack of 10 highest ranked nodes based on degree of connectivity. Figures 6a, 6b, and 6c show that node failures are worse than link attacks or failures, since each node failure is equivalent of the failure of all links incident to that node. Our results indicate that attacks launched with knowledge of the network topology can cause the most severe degradation. We can also infer the trade-off between robustness and cost of building topologies using our framework.

B. Area-based Challenges

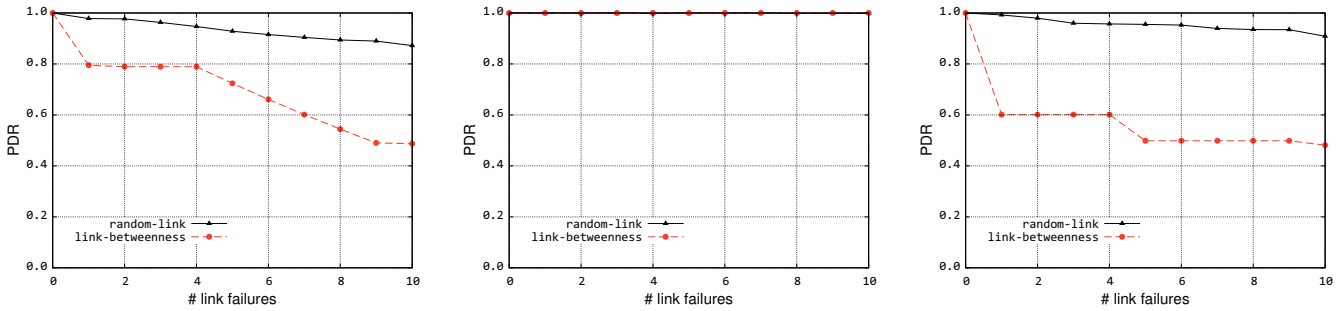
As previously discussed, our framework uses circles or polygons to model geographically correlated failures representative of large-scale disasters needed for network survivability [5], [30]. Area-based challenges in our model can be stationary or evolving in time. Next, we present the results of three scenarios that demonstrate area-based challenges that evolve spatially and temporally. In all scenarios, as shown in Figure 7, we use the Rocketfuel inferred Sprint topology as shown in Figure 4a. Application traffic is generated from 2 to 29 sec. and challenge scenarios were applied from 10 until 22 sec. for the performance plots as shown in Figure 8.

1) Scaling circle: To demonstrate a scaling circle area-based challenge scenario, we simulate a circle centered at $(-74.00\,^\circ, 40.71\,^\circ)$, in New York, USA as shown in Figure 7a, with a radius of $1\,^\circ$ (approximately 111 km). We choose the scenario to be representative of an electromagnetic pulse (EMP) attack [31]. The PDR is shown in Figure 8a. We choose the simulation parameters such that the radius doubles in every 4 sec. As can be seen, the PDR reduces as the circular area doubles. The PDR drop depends on how many nodes and links resides in the each step.

2) Moving circle: Next, we demonstrate an area-based scenario that can evolve spatially and temporally. We simulate a moving circle in a trajectory from Orlando, USA $(-81.37\,^\circ,$

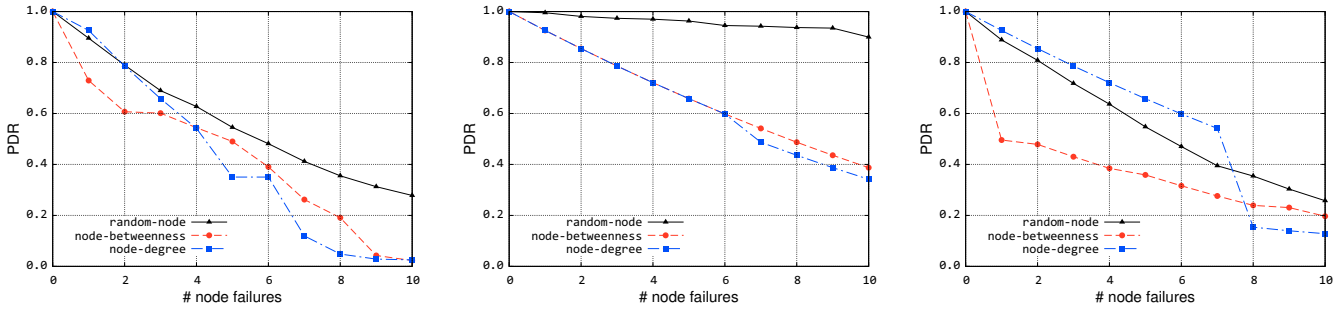
(a) Sprint inferred topology (b) Synthetic topology 1 (c) Synthetic topology 2

Fig. 4. Sample topologies for evaluation of node and link failures



(a) Sprint inferred topology (b) Synthetic topology 1 (c) Synthetic topology 2

Fig. 5. PDR during non-malicious and malicious link perturbations



(a) Sprint inferred topology (b) Synthetic topology 1 (c) Synthetic topology 2

Fig. 6. PDR during non-malicious and malicious node perturbations

28.53 °) to New York, USA (−74.00 °, 40.71 °). Three snapshots of the evolving challenge are shown in Figure 7b. The radius of the circle is kept at 2 ° (approximately 222 km). We choose the simulation parameters for illustration such that the circle reaches NY in seven seconds (to constrain simulation time), with route recomputation every 3 sec.

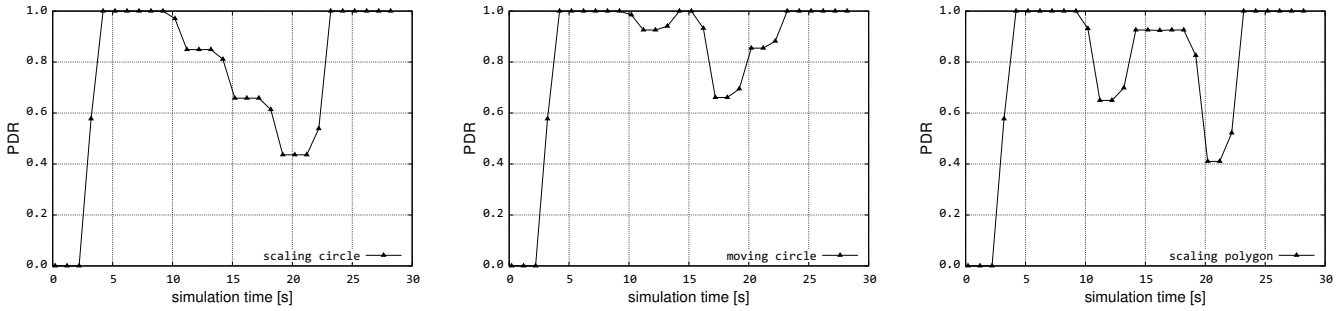
As shown in Figure 8b PDR reduces to 93% as the challenge starts only covering the node in Orlando at 10 sec. As the challenge moves towards NY in its trajectory, the PDR reaches one at the 13 sec. In this case, the challenge area includes only the link between Orlando and NY, but since there are multiple paths a single link failure does not affect the PDR, showing that *diversity for survivability* is crucial [1]. As the challenge moves into the northeast US region at 16 sec., the PDR drops to 66% as the challenge covers several nodes and links. The simulation shows that as the circle moves out of the more crowded region of the network, the PDR improves, until the challenge is ended at the 22 sec.

3) Scaling polygon: Polygons are useful to model specific geographic challenges such as power failures. For a scaling polygon example, we show a 6-sided irregular polygon in the Midwest region of the US, roughly representative of the North American Electric Reliability Corporation (NERC) Midwest region [31], with vertices at: [(−87.91 °, 43.04 °), (−89.09 °, 42.27 °), (−89.64 °, 39.8 °), (−88.54 °, 39.12 °), (−88.24 °, 40.12 °), (−87.65 °, 41.85 °)] as shown in Figure 7c.

The PDR throughout the simulation is shown in Figure 8c. In this scenario, the edges of the irregular polygon increase 1.8

(a) Scaling circle (b) Moving circle (c) Scaling polygon

Fig. 7. Area-based challenge scenarios



(a) Scaling circle PDR (b) Moving circle PDR (c) Scaling polygon PDR

Fig. 8. PDR during area-based challenges

times every three sec. At 10 sec. the challenge affects 16 links, which causes the PDR to drop to 65%. The PDR then increases to 93%, even though more links and nodes are affected at 13 sec. because of route reconvergence. As the polygon increases in size, the PDR drops to as low as 41%, because the challenge area partitions the network at 21 sec. This type of scenario can be used either to understand the relationship between the area of a challenge and network performability, or to model a temporally evolving challenge, such as a cascading power failure that increases in scope over time.

C. Wireless Domain Challenges

Wireless challenges are modelled as jammers and impairments in our ns-3 framework as discussed in Section III. In this section, we present a scenario that combines both types of challenges. In this scenario, a jammer node and impairment move as shown in Figure 9. The sender is located at coordinate (300,0), the receiver is located at (0,0), and the jammer node is located at (-100,0). During the simulation the impairment sweeps across the wireless network from left to right horizontally.

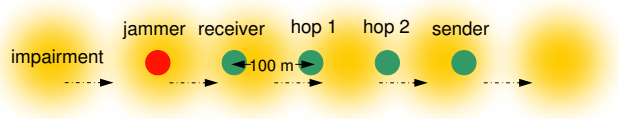


Fig. 9. Jammer and impairment combined scenario

The performance result of the above scenario is shown in Figure 10. In this scenario, the jammer is set up so that it will cause 70% packet loss for the legitimate traffic between the sender and the receiver. As the impairment sweeps horizontally, the PDR changes accordingly. In the region when the impairment affects the jammer node, 100% PDR is achieved between the sender and the receiver. As the impairment affects the receiver or sender, the PDR drops to 0%.

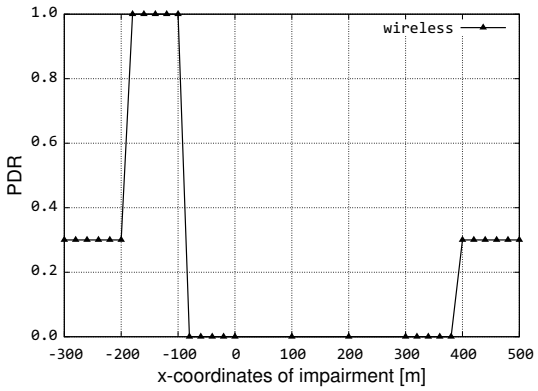


Fig. 10. PDR for wireless challenge scenario

It should be noted that for the wireless domain challenges, a jammer's mobility pattern can cause either random or targeted attacks, depending on intentional placement near a critical node vs. a jammer with a random mobility pattern.

V. Conclusions and Future Work

Understanding the challenges faced by the networks that are inherent in the communication environment is crucial for understanding the network behaviour. We presented modelling of these challenges and how they can be categorised. Also, we presented a comprehensive framework to evaluate the network performance when faced by realistic stationary or evolving challenges that can spatially or temporally change, which separates network topology from challenge specification. Our results indicate the network performance varies depending on the type and severity of the challenge applied. On the other hand, these results validate our methodology.

This paper has concentrated on illustrating the basic functionality of our challenge framework to demonstrate its utility in understanding network resilience. Future work will consist of applying this framework to a variety of real and synthetic wired, wireless, and mixed topologies to better understand the resilience of existing and future networks. Furthermore, we will begin to apply this methodology to a large-scale testbed with emulated challenges, using the GpENI (Great Plains Environment for Network Innovation) [2] testbed.

Acknowledgments

We would like to acknowledge Justin P. Rohrer, Abdul Jabbar, and other members of the ResiliNets group for discussions on this work. This research was supported in part by NSF FIND (Future Internet Design) Program under grant CNS-0626918 (Postmodern Internet Architecture) and by the EU FP7 FIRE programme ResumeNet project (grant agreement no. 224619).

References

[1] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[2] J. P. Sterbenz, D. Medhi, B. Ramamurthy, C. Scoglio, *et al.*, "The Great Plains Environment for Network Innovation (GpENI): A programmable testbed for future internet architecture research," in *Proc. of the 6th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (TridentCom)*, May 2010.

[3] D. Nicol, W. Sanders, and K. Trivedi, "Model-based evaluation: from dependability to security," *IEEE Trans. on Dependable and Secure Comp.*, vol. 1, no. 1, pp. 48–65, 2004.

[4] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. on Dependable and Secure Comp.*, vol. 1, no. 1, pp. 11–33, 2004.

[5] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R. Ramanathan, and J. Zao, "Survivable mobile wireless networks: issues, challenges, and research directions," in *Proc. of ACM WiSe*, pp. 31–40, 2002.

[6] H. Daugherty and W. Klein, "US network reliability issues and major outage performance," in *Proc. of ISCC*, pp. 114–119, 1995.

[7] D. Kuhn, "Sources of failure in the public switched telephone network," *IEEE Computer*, vol. 30, no. 4, pp. 31–36, 1997.

[8] D. Oppenheimer, A. Ganapathi, and D. A. Patterson, "Why do internet services fail, and what can be done about it?," in *Proc. of USENIX USITS*, pp. 1–16, 2003.

[9] G. O'Reilly, A. Jrad, R. Nagarajan, T. Brown, and S. Conrad, "Critical infrastructure analysis of telecom for natural disasters," in *Proc. of IEEE Networks*, pp. 1–6, 2006.

[10] Y. Kitamura, Y. Lee, R. Sakiyama, and K. Okamura, "Experience with Restoration of Asia Pacific Network Failures from Taiwan Earthquake," *IEICE Trans. on Comm.*, vol. 90, no. 11, pp. 3095–3103, 2007.

[11] "Severe space weather events: Understanding societal and economic impacts," workshop report, National Research Council, 2008.

[12] J. Laprie, K. Kanoun, and M. Kaaniche, "Modelling interdependencies between the electricity and information infrastructures," *LNCS*, vol. 4680, pp. 54–67, 2007.

[13] J. H. Cowie, A. T. Ogielski, B. Premore, E. A. Smith, and T. Underwood, "Impact of the 2003 blackouts on internet communications," tech. rep., Renesys Corporation, 2003.

[14] A. Jabbar, J. Rohrer, A. Oberthaler, E. Çetinkaya, V. Frost, and J. Sterbenz, "Performance comparison of weather disruption-tolerant cross-layer routing algorithms," in *Proc. of IEEE INFOCOM*, pp. 1143–1151, 2009.

[15] "The ns-3 Network Simulator." http://www.nsnam.org/.

[16] N. Spring, R. Mahajan, and D. Wetherall, "Measuring ISP topologies with Rocketfuel," in *Proc. of ACM SIGCOMM*, pp. 133–145, 2002.

[17] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, "Resilience of the internet to random breakdowns," *Phys. Rev. Lett.*, vol. 85, pp. 4626–4628, Nov 2000.

[18] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: Percolation on random graphs," *Phys. Rev. Lett.*, vol. 85, pp. 5468–5471, Dec 2000.

[19] P. Mahadevan, D. Krioukov, M. Fomenkov, X. Dimitropoulos, K. C. Claffy, and A. Vahdat, "The Internet AS-level topology: three data sources and one definitive metric," *ACM SIGCOMM CCR*, vol. 36, no. 1, pp. 17–26, 2006.

[20] S.-T. Park, A. Khrabrov, D. Pennock, S. Lawrence, C. Giles, and L. Ungar, "Static and dynamic analysis of the internet's susceptibility to faults and attacks," in *Proc. of IEEE INFOCOM*, vol. 3, pp. 2144–2154, 2003.

[21] J. Doyle, D. Alderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger, "The robust yet fragile nature of the Internet," *PNAS*, vol. 102, no. 41, pp. 14497–14502, 2005.

[22] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E*, vol. 65, p. 056109, May 2002.

[23] A. Sydney, C. Scoglio, M. Youssef, and P. Schumm, "Characterizing the robustness of complex networks," *Int. J. Internet Technology and Secured Transactions*, 2010. to appear.

[24] "CGAL, Computational Geometry Algorithms Library." http://www.cgal.org.

[25] B. Bassiri and S. S. Heydari, "Network survivability in large-scale regional failure scenarios," in *Proc. of ACM C3S2E*, pp. 83–87, 2009.

[26] I. Chatzigiannakis, A. Kinalis, G. Mylonas, S. Nikoletseas, G. Prasinos, and C. Zaroliagis, "TRAILS, a Toolkit for Efficient, Realistic and Evolving Models of Mobility, Faults and Obstacles in Wireless Networks," in *Proc. of 41st Annual Simulation Symposium*, pp. 23–32, 13-16 April 2008.

[27] M. A. Hameed, A. Jabbar, E. K. Çetinkaya, and J. P. Sterbenz, "Deriving Network Topologies from Real World Constraints," in *Proc. of IEEE GLOBECOM Workshop on Complex and Communication Networks (CCNet)*, 2010. to appear.

[28] A. Jabbar, Q. Shi, E. Çetinkaya, and J. P. Sterbenz, "KU-LocGen: Location and cost-constrained network topology generator," ITTC Technical Report ITTC-FY2009-TR-45030-01, The University of Kansas, Lawrence, KS, December 2008.

[29] B. Waxman, "Routing of multipoint connections," *IEEE Journal on Selected Areas in Communications*, vol. 6, no. 9, pp. 1617–1622, 1988.

[30] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead, "Survivable network systems: An emerging discipline," Tech. Rep. CMU/SEI-97-TR-013, Carnegie-Mellon Sorfware Engineering Institute, PA, 1999.

[31] "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," report, Critical National Infrastructures, 2004.